Testimony of

Michael M. Meldon
Executive Director
Homeland Security & Defense Business Council

Joint Hearing of the House Committee on Homeland Security's
Subcommittee on Management, Integration, and Oversight and
Emergency Preparedness, Science, and Technology

Helping Business Protect the Homeland:
Is the Department of Homeland Security Effectively Implementing the SAFETY Act?

September 13, 2006

Good afternoon, Chairman Rogers, Chairman Reichert, and distinguished members of the subcommittee. My name is Michael Meldon and I am the Executive Director of the Homeland Security and Business Council. I am testifying on behalf of our member companies. The Homeland Security & Defense Business Council is a non-profit, non-partisan organization that represents good governance and successful program outcomes. The Council offers "straight talk" and honest assessments of programs, technology, and processes that are integral to the mission of the Department of Homeland Security. The Council's goal is to be a world class private sector component and partner to the public sector in all significant areas of homeland security to include risk mitigation, mission effectiveness, and management efficiency.

The Council appreciates the opportunity to present our industry perspective on the SAFETY Act Final Rule recently released by the Department of Homeland Security.

There are a number of very positive changes that have occurred in the business processes and guidelines surrounding the SAFETY Act. To highlight some of these, the final rule makes these changes to the Safety Act:

- **Provides that a technology includes services as well as equipment and software.** This means maintenance contractors may be entitled to liability protection if they service equipment used for anti-terrorism purposes, or if they provide design, consulting, analysis or other professional services.

- **Removes the need for anti-terrorism technology sellers to offer insurance coverage to third persons for acts of suppliers, vendors and subcontractors used to supply the technology.** This expands the bargain struck in the Safety Act, which exchanged limitations on the seller's legal liability to the public for a requirement that the seller get liability insurance coverage.

- **Lets a seller of a qualified anti-terrorism technology make changes to the product that modify its capabilities without approval by, or even notice to, DHS, and without loss of the liability projections provided by the Safety Act.** Under the interim rule, a seller that made significant modifications to the technology that reduced its capabilities could lose its liability protection as of the time the change was made. Under the final rule, however, if the product modification is so significant that the product would no longer qualify for liability protection, and then the seller is required to give notice to DHS. The product retains the liability protections until DHS takes affirmative steps to terminate its qualification.

- **Grants DHS the right to create so-called block designations and certifications for certain categories of anti-terrorism technologies.** Sellers whose technologies fall within these will not have to demonstrate their technology's technical merits. They will be entitled to receive the liability protections simply

by submitting an abbreviated application showing that the technology is covered by the pre-approved block determination.

- **Addresses DHS' policy on safeguarding proprietary information regarding applications for anti-terrorism designation and certification.**

The new rule also addresses the application evaluation timeliness issues we have seen from an industry perspective. The information provided in the Department's announcement of the Final Rule (6 CFR Part 25, [USCG-2003-15425]/RIN 1601-AA15) states that in the first 16 months following the passage of the SAFETY Act, 6 QATT's were approved and an additional 68 technologies were approved by March 2005. What this does not address is the number of applications (thought to be in the hundreds) that have been received by the Department for which no action has been taken.

Several issues remain in the SAFETY Act and its intended implementation and I will focus the remainder of my time on these issues.

Anticipated changes in the insurance industry

The SAFETY Act was designed to encourage firms to bring homeland security products to market by eliminating the "bet-your-company" risk that might turn some of them away. Insurance companies and the federal government paid more than 90 percent of the $38.1 billion awarded to victims of the Sept. 11 terrorist attacks, according to a 2004 study by the nonprofit RAND Corp. Because of concerns about an avalanche of claims, Congress capped liability for airlines, airports, ports and cities and established the Sept. 11 Victim Compensation Fund of 2001. To use it, recipients had to waive their right to sue. Still, about 70 families eventually filed wrongful death suits against airlines. Plaintiffs also sued the former Riggs Bank - alleging that lax oversight facilitated the financing of two hijackers - and 12 families of firefighters sued Motorola Inc. and New York City over faulty hand-held radios. That suit later was thrown out of court. The nature of these suits and the potential liability exposure was closely examined by the insurance industry as well as others and the business considerations that resulted from their review are being implemented through new policy terms and conditions.

Thankfully, the United States has not suffered a terrorist attack, or resulting lawsuits, since the fall of 2001, so the protections of the SAFETY Act haven't come into play. But industry's concern about liability is no less real. Large contractors bolstering the blast-resistance of bridges, ports and other hard targets; system integrators designing buildings and technological systems; manufacturers of infrared cameras and motion detectors on the border; and biotech firms supplying vaccines all could face lawsuits after a terrorist attack.

Government Contractor Defense

Implementation and guidance regarding the Government Contractor Defense is noted in the Final Rule as an area that DHS still owes industry specific direction and policies/procedures.

The presumption of the government contractor defense applies to all "approved" qualified anti-terrorism technologies for all claims brought in any kind of lawsuit "arising out of, relating to, or resulting from an act of terrorism when qualified anti-terrorism technologies . . . have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller." While the government contractor defense is a judicially created doctrine requiring the Contractor/Provider to prove essential elements in order to qualify for the defense, the SAFETY Act supplants the case law so that once the Secretary "approves" the application for this additional protection, the government contractor defense applies.

Significantly, the statutory government contractor defense available under the SAFETY Act provides immunity not only against all claims that might be brought by third parties relating to sales to the government, it also applies to purely private transactions. Thus, once the Secretary "approves" a qualified anti-terrorism technology for this additional protection, the Contractor/Provider is immune from liability relating to sales of that technology in the commercial sector.

Moreover, under the case law, the government contractor defense is available only if the contractor manufactured the product in question in accordance with reasonably precise federal government specifications. Under the SAFETY Act, that is not the case. In reviewing an application, the Secretary will perform a "comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended." The Act also provides that the Seller will "conduct safety and hazard analyses" and supply such information to the Secretary.

Thus, unlike the existing judicially created government contractor defense, the DHS statutory government contractor defense will protect Contractor/Providers of technology in the commercial marketplace and will allow qualified anti-terrorism technologies to be approved for such treatment even if a federal specification is not involved.

The proposed rule clearly adopts the broad protections provided by the case law to the SAFETY Act's version of the government contractor defense. The proposed rule recognizes that the scope of the defense is very broad, and expressly states that Sellers of "approved" qualified anti-terrorism technologies cannot be held liable under the SAFETY Act for design defects or failure to warn claims (unless the presumption is established through evidence that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary in connection with its application).
As noted above, applications to gain this protection may be submitted simultaneously with the application for "designation" as a qualified anti-terrorism technology. The

immunity provided by the statutory government contractor defense is a remarkable protection afforded to sellers of anti-terrorism technologies, and we expect most sellers of such technologies to submit applications.

The court and case law test of DHS' interpretation will unfortunately be played out against another tragedy (hopefully averted) and the use of the DHS statutory rule which may come under pressure since it departs from the current PL 85-804.

Exclusive Federal Jurisdiction and Scope of Insurance Coverage

The Final Rule establishes that before the Secretary may designate a technology as a qualified anti-terrorism technology, he must examine the amount of liability insurance the Seller intends to maintain for coverage of the technology and certify that the coverage level is appropriate to satisfy otherwise compensable third-party claims that may be caused by an act of terrorism when qualified anti-terrorism technologies have been implemented. The SAFETY Act also provides that Contractor/Providers are not required to obtain insurance in excess of the maximum amount reasonably available that would not unreasonably distort the sales price of the anti-terrorism technology.

The rule states that the Secretary does not intend to set a numerical "one-size-fits-all" level of insurance requirement for all technologies. Instead, the required level of insurance will be determined on an application-by-application basis and will be based upon the examination of several factors, including: "the amount of insurance the Contractor/Provider has previously maintained; the amount of insurance maintained for other technologies or for the business as a whole; the amount of insurance typically maintained by sellers of comparable technologies; data and history regarding mass casualty losses; and the particular technology at issue." The rule also suggests that the Secretary might confer with the Contractor/Providers, and insurance carriers, to determine the appropriate level of insurance to require for a particular application. The proposed rule recognizes that over time the appropriate level of insurance may change based on the market for insurance, the predominance of a particular threat, and other factors. Accordingly, the Contractor/Provider is allowed to seek reconsideration of the insurance required.

The impact for not maintaining the required level of insurance are also addressed in the rule. If a Contractor/Provider allows its insurance to fall below the required level of insurance, the protections of the SAFETY Act will still apply. However, the maximum liability of the Contractor/Provider remains at the required level of insurance so they may be subjecting itself to an uninsured liability. In addition, allowing the insurance to fall below the required level will be regarded as a negative factor by the Secretary for any future application for renewal of the SAFETY Act protections and might be considered as a negative factor for any other SAFETY Act applications submitted by the same Contractor/Provider.

Confidentiality of Information

Under the Freedom of Information Act, Trade Secrets Act and other federal statutes, trade secrets and other proprietary information submitted to DHS by an applicant remain confidential. In the final rule, however, DHS has taken the position that all information submitted by an applicant, whether or not proprietary or a trade secret and including the applicant's identity, will be withheld from disclosure.

The breadth of the information that DHS may withhold is subject to debate, and DHS has staked out an aggressive position. Parties submitting applications for anti-terrorism technology designation or certification still should be careful because courts frequently have taken a more nuanced view of the proper balance between protecting commercially valuable information and the public's right to examine the decisions of its government agencies.

Certifying "accuracy and completeness"

The standard for performance of this final rule clause is almost impossible to determine – yet the industry case will rest heavily on the process that led them to seek the QATT in the first place. The parameters used for "accuracy and completeness" are also likely to be used in determining negligence or fraud. Since DHS is not dealing with a detailed federal government specification for defined products, services and support the method for certifying "accuracy and completeness" remains subjective.

Significant Modification to a Qualified Anti-Terrorism Technology

The final rule discusses the provisions of ongoing modification to QATT in service. The issue that this raises, however, deals with QATT that has undergone in place upgrades and enhancements without specific DHS review. The worst case scenario suggests that DHS could develop a finding that determines that a product thought to be on the QATT and covered with appropriate liability insurance, is not and a fraud has occurred. Third parties in this scenario then have additional options to recover from claims. However horrific it seems, the potential test of this rule could be in the aftermath of a significant terrorist attack on the US and the availability of 'clear and convincing evidence' to support claims against a Seller may not be possible.

Scope of Insurance Coverage

The final rule creates a single cause of action with exclusive jurisdiction in a federal district court. As a result, we might expect to see plaintiffs suing in foreign countries whenever possible to avoid the liability limitations of the Act. Industry will be carefully considering appropriate corporate structures necessary to ameliorate this possibility and to keep federal causes of action in the United States.

Reconsideration of Designations

The final rule also suggests that a designation as a qualified anti-terrorism technology will last for five to eight years and may be renewed, but seeks comment on this proposed duration. The SAFETY Act does not contain any time limit on the length of the "designation." There appears to be no logical reason why there should be any time-based limitation on the designation as a QATT - a technology that meets the criteria today and is afforded the protections of the statute, should be eligible for the same protection so long as the technology is available and in service.